ABSTRACT

A METHOD OF PROTECTING A CRYPTOGRAPHIC ALGORITHM

The method of protecting an algorithm that can be decomposed into the form of initial polynomials (P_i) of at least two variables and of degree not less than two, comprises the steps of making combined polynomials (Q_k) each obtained from at least two initial polynomials (P_i, P_{i+1}), and of storing the combined polynomials (Q_k) in the form of a configuration file in a memory (3) associated with a processor unit (4).

Translation of the title and the abstract as they were when originally filed by the Applicant. No account has been taken of any changes that may have been made subsequently by the PCT Authorities acting ex officio, e.g. under PCT Rules 37.2, 38.2, and/or 48.3.